**3GPP TSG-SA3 Meeting SA3#110-adhoc-e *S3-23xxxx***

**Electronic meeting, 17 - 21 April 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **draft-CR** | **rev** | **-** | **Current version:** | **18.1.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  |  Skeleton for Security aspects of enhanced support of Non-Public Networks phase 2 |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eNPN\_Ph2 |  | ***Date:*** | 2023-04-10 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** |  |
|  |  |
| ***Summary of change:*** | Skeleton for how work on Security aspects of enhanced support of Non-Public Networks phase 2 can be included in TS 33.501. The sub-clause headings are aligned with the sub-clause headings in clause 5.30.2 of TS 23.501. |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\* BEGIN CHANGES \*\*\*

Annex I (normative):
Non-public networks

# I.1 General

This Annex provides details on security for non-public networks. Most of the security procedures are the same as public networks so this annex only summarizes and specifies where there are exceptions to the normal procedures.

The feature for support of non-public networks (NPN) by 5GS is described in clause 5.30 of 23.501 [2].

# I.2 Authentication in standalone non-public networks

## I.2.1 General

One of the major differences of non-public networks is that authentication methods other than AKA based ones may be used in a standalone non-public network (SNPN). When an AKA-based authentication method is used, clause 6.1 shall apply. When an authentication method other than 5G AKA or EAP-AKA' is used, only the non-AKA specific parts of clause 6.1 shall apply. An example of running such an authentication method is given in Annex B with EAP-TLS.

The choice of the supported authentication methods for access to SNPNs follows the principles described in clauses I.2.2 and I.2.3.

The authentication server can be an internal authentication server or an external authentication server. The internal authentication server is the AUSF, and the authentication method can be 5G-AKA or EAP-AKA´ as described in clause 6.1, or can be EAP-TLS as described in Annex B. When external authentication server is the AAA, the primary authentication procedure is described in Annex I.2.2.2.2. When external authentication server is an AUSF, then the primary authentication procedure is described in Annex I.2.4. The UDM decides to run primary authentication with internal authentication server or external authentication server.

## I.2.2 EAP framework, selection of authentication method, and EAP method credentials

### I.2.2.1 General

The EAP authentication framework is supported by the 5GS as described in clause 6.1.1.2.

The UE and the SNPN may support 5G AKA, EAP-AKA', or any other key-generating EAP authentication method.

Selection of the authentication methods is dependent on NPN configuration.

NOTE 1: For EAP-AKA' (as well as 5G AKA), the selection is described in clause 6.1.2. For authentication, that is not using EAP-AKA' (or 5G AKA), the selection is NPN operator deployment specific and out of scope of this specification.

When an EAP authentication method other than EAP-AKA' is selected, the chosen method determines the credentials needed in the UE and network. These credentials, called the EAP-method credentials, shall be used for authentication.

NOTE 2: How credentials for EAP methods other than EAP-AKA' are stored and processed within the UE is out of the scope for standalone non-public networks.

NOTE 3: Storage and processing of credentials for EAP-AKA' (as well as 5G AKA) is described in clause 6 of the present document.

### I.2.2.2 Credentials holder using AAA server for primary authentication

#### I.2.2.2.1 General

The procedures described in this clause enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN.

In this scenario the authentication server role is taken by the AAA Server. The AUSF acts as EAP authenticator and interacts with the AAA Server to execute the primary authentication procedure.

The architecture for SNPN access using credentials from a Credentials Holder using AAA Server is described in clause 5.30.2.9.2 of TS 23.501 [2].

#### I.2.2.2.2 Procedure



Figure: I.2.2.2.2-1: Primary authentication with external domain

0. The UE shall be configured with credentials from the Credentials holder e.g. SUPI containing a network-specific identifier and credentials for the key-generating EAP-method used. As part of configuration of the credentials, the UE shall also be configured with an indication that the UE shall use MSK for the derivation of KAUSF after the success of the primary authentication. The exact procedures used to configure the UE are not specified in the present document.

 It is further assumed that there exists a trust relation between the SNPN and the Credentials holder AAA Server. These entities need to be mutually authenticated, and the information transferred on the interface need to be confidentiality, integrity and replay protected.

When the procedures of this clause are used for onboarding purposes, the onboarding specific adaptations includes: the 'credentials' used is 'Default credentials', the 'SUPI' used is 'onboarding SUPI', the 'SUCI' used is 'onboarding SUCI' respectively.

1. The UE shall select the SNPN and initiate UE registration in the SNPN.

 For construction of the SUCI, existing methods in clause 6.12 can be used. Otherwise, if the EAP method supports SUPI privacy, the UE may send an anonymous value SUCI based on configuration.

2. The AMF within the SNPN shall initiate a primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF. The AMF shall discover and select an AUSF based on criterions specified in TS 23.501 [2] clause 5.30.2.9.2.

3. In the case of onboarding, steps 3-5 are omitted. If steps 3-5 are not omitted, the AUSF shall initiate a Nudm\_UEAuthentication\_Get service operation. The AUSF shall discover and select a UDM based on criterions specified in TS 23.501 [2] clause 5.30.2.9.

NOTE 1: SUPI will be used instead of SUCI in the case of a re-authentication.

4. In case the UDM receives a SUCI, the UDM shall resolve the SUCI to the SUPI before checking the authentication method applicable for the SUPI. The UDM decides to run primary authentication with an external entity based on subscription data.

In case the UDM receives an anonymous SUCI, the UDM decides to run primary authentication with an external entity based the realm part of the SUPI in NAI format.

NOTE 1a: The UDM needs to be configured with a list of realms and the intended authentication server

 In case the UDM receives an anonymous SUCI that does not contain the realm part, the UDM shall abort the procedure. Otherwise, the UDM authorizes the UE based on realm part of SUCI and send the anonymous SUPI and the indicator to the AUSF as described in step5.

 The anonymous SUPI shall be a NAI format.

5. In case the UDM received a SUCI in previous steps, the UDM shall provide the AUSF with the SUPI or anonymous SUPI and shall indicate to the AUSF to run primary authentication with a AAA Server in an external Credentials holder.

 When a Credentials Holder using AAA Server is used for primary authentication, the AUSF uses the MSK to derive KAUSF. It is strongly recommended that the same credentials that are used for authentication between UE and the 5G SNPN are not used for the authentication between the UE and a non-5G network, assuming that 5G SNPN and non-5G network are in different security domains.

NOTE 2: MSKs obtained from the non-5G network could be used to impersonate the 5G SNPN towards the UE.

6. Based on the indication from the UDM, the AUSF shall select an NSSAAF as defined in TS 23.501 [2] and initiate a Nnssaaf\_AIWF\_Authenticate service operation towards that NSSAAF as defined in clause 14.4.2.

7. The NSSAAF shall select AAA Server based on the domain name corresponding to the realm part of the SUPI. The NSSAAF shall perform related protocol conversion and relay EAP messages to the AAA Server.

NOTE 3: The interface and protocol between NSSAAF and AAA is out of scope of the present document and existing AAA protocols such as RADIUS or Diameter can be used.

8. The UE and AAA Server shall perform mutual authentication. The AAA Server shall act as the EAP Server for the purpose of primary authentication. The EAP Identity received by the AAA Server in the EAP-Response/Identity message in step 7 may contain anonymised SUPI. In such cases, AAA Server uses the EAP-method specific EAP Identity request/response messages to obtain the UE identifier as part of the EAP authentication between the UE and the AAA Server.

9. After successful authentication, the MSK and the SUPI (i.e., the UE identifier that is used for the successful EAP authentication) shall be provided from the AAA Server to the NSSAAF.

10. The NSSAAF returns the MSK and the SUPI to the AUSF using the Nnssaaf\_AIWF\_Authenticate service operation response message. The SUPI received from the AAA shall be used when deriving 5G keys (e.g., KAMF) that requires SUPI as an input for the key derivation.

11-13. In case of onboarding or SUCI received in step 2 is not anonymous, steps 11-13 are omitted. Otherwise, the AUSF verifies that the SUPI corresponds to a valid subscription in the SNPN by informing the UDM about the authentication result for the received SUPI using a Nudm\_UEAuthentication\_ResultConfirmation service operation. The UDM stores the authentication state for the SUPI and if there is not a subscription corresponding to the SUPI, the UDM shall return an error.

If the verification of the SUPI is not successful, then the AUSF rejects the UE access to the SNPN.

NOTE 4: If the above failure happens, the error is no failed authentication but lacking subscription in the SNPN.

14. The AUSF shall use the most significant 256 bits of MSK as the KAUSF. The AUSF shall also derive KSEAF from the KAUSF as defined in Annex A.6.

15. The AUSF shall send the successful indication together with the SUPI of the UE to the AMF/SEAF together with the resulting KSEAF.

16. The AMF shall send the EAP success in a NAS message.

17. The UE shall derive the KAUSF from MSK as described in step 11 according to the pre-configured indication as described in step 0.

## I.2.3 Key hierarchy, key derivation and key distribution

### I.2.3.1 General

The text in clauses 6.2.1 and 6.2.2 cannot apply directly for an EAP authentication method other than EAP-AKA' as these clauses assume that an AKA-based authentication method is used. The major differences are the way in which KAUSF is calculated and that the UDM/ARPF is not necessarily involved in the key derivation or distribution.

Depending on the selected authentication method, the KAUSF is generated as follows:

- For 5G AKA and EAP-AKA' refer to clause 6.2.1.

- When using a key-generating EAP authentication method other than EAP-AKA', the key derivation of KAUSF is based on the EAP-method credentials in the UE and AUSF and shall be done as shown in Figure I.2.3-1.

NOTE: For EAP authentication methods other than EAP-AKA', this key derivation replaces clauses 6.2.1 and 6.2.2 for the generation of KAUSF .



Figure I.2.3.1-1: KAUSF derivation for key-generating EAP authentication methods other than EAP-AKA'

KAUSF shall be derived by the AUSF and UE from the EMSK created by the EAP authentication as for EAP-AKA'.

All of figures 6.2.1-1, 6.2.2.1-1 and 6.2.2.2.2-1 from the KAUSF downwards are used without modification. Similarly, text relating to the key hierarchy, key derivation and key distribution in clauses 6.2.1, 6.2.2.1 and 6.2.2.2 for keys derived from KAUSF (e.g. KSEAF, KAMF, KgNB etc) apply without modification.

### I.2.3.2 Credentials holder using AAA server for primary authentication

When running primary authentication towards an external Credentials holder using AAA server for authentication as specified in clause I.2.2.2 the derivation of KAUSF is based on the EAP-method credentials in the UE and AAA-S and shall be done as shown in Figure I.2.3.2-1.



Figure I.2.3.2-1: KAUSF derivation for primary authentication towards an external Credentials holder using AAA server

KAUSF shall be derived by the AUSF and UE from the MSK derived during the EAP authentication as specified in clause I.2.2.2.1.

All of figures 6.2.1-1, 6.2.2.1-1 and 6.2.2.2.2-1 from the KAUSF downwards are used without modification. Similarly, text relating to the key hierarchy, key derivation and key distribution in clauses 6.2.1, 6.2.2.1 and 6.2.2.2 for keys derived from KAUSF (e.g. KSEAF, KAMF, KgNB etc) apply without modification.

### I.2.4 Credentials Holder using AUSF and UDM for primary authentication

The 5G System architecture for SNPN with Credentials Holder using AUSF and UDM for primary authentication and authorization is described in clause 5.30.2.9.3 of TS 23.501 [2].

The requirements and procedures for primary authentication using AUSF and UDM as described in the present document apply, for 5G AKA, EAP-AKA', EAP-TLS or any other key-generating EAP method.

# I.3 Serving network name for standalone non-public networks

## I.3.1 General

The identification of standalone non-public networks uses Network Identifier (NID) in addition to PLMN ID. This means the definition of SN Id in clause 6.1.1.4.1 for the derivation of KSEAF for all authentication methods, CK' and IK' for EAP-AKA', and KAUSF and (X)RES\* for 5G AKA needs modification for standalone non-public networks.

## I.3.2 Definition of SN Id for standalone non-public networks

For standalone non-public networks, the SN Id (used in the input for various key/parameter derivations) identifies the serving SNPN.

It is defined as follows:

SN Id = PLMN ID:NID

and is specified in detail in TS 24.501 [35].

# I.4 Modification of CAG ID list in the UE

The following requirements apply to NAS messages that modify the list of CAG IDs stored in the UE:

- the AMF shall only send such a NAS message once NAS security has been established; and

- the UE shall only modify its list of CAG IDs after successful integrity verification of the integrity protected NAS message requesting such a modification.

# I.5 SUPI privacy for standalone non-public networks

The UE shall support SUPI privacy as defined in clause 6.12 with the following exception. When using an authentication method other than 5G AKA or EAP-AKA', the location of the functionality related to SUPI privacy in the UE is out of scope.

In scenarios where the EAP-method supports privacy, the UE may send an anonymous SUCI based on configuration.

Furthermore, the privacy considerations for EAP TLS (given in Annex B.2.1.2) should be taken into account when using an authentication method other than 5G AKA or EAP-AKA'.

# I.6 Authentication in Public Network Integrated Non-Public Networks (PNI-NPN)

For public network integrated NPN (PNI-NPN), the primary authentication shall be performed with the public network as described in clause 6.1. Secondary authentication as described in clause 11 and slice-specific authentication as described in the main body can take place after a successful primary authentication.

# I.7 Authorization aspects in SNPNs

## I.7.1 Credentials holder using AUSF and UDM for primary authentication

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, service authorization as specified in clause 13.4.1.2 applies.

# I.8 SEPP and interconnect related security procedures

## I.8.1 Credentials holder using AUSF and UDM for primary authentication

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, clause 5.30.2.9.3 of TS 23.501 [2] states that the UE is not considered to be roaming, however SNPN and Credentials Holder communicate via SEPPs.

The following requirements and procedures related to SEPPs and interconnect security apply for SNPNs with Credentials Holder using AUSF and UDM for primary authentication:

- Requirements for Security Edge Protection Proxy (SEPP), clause 5.9.3.2

- Protection between SEPPs, clause 13.1.2.

NOTE: IPX providers are not expected to be used between SNPN and Credentials holder using AUSF and UDM for primary authentication.

# I.9 Security of UE onboarding in SNPNs

## I.9.1 General

Onboarding of UEs for SNPNs is specified in clause 5.30.2.10 of TS 23.501 [2].

Onboarding of UEs for SNPNs allows the UE to access an Onboarding Network (ONN) based on Default UE credentials for the purpose of provisioning the UE with SNPN credentials and any other necessary information. The Default UE credentials are pre-configured on the UE. Default UE credentials consist of credentials for primary authentication and optionally credentials for secondary authentication.

To provision SNPN credentials in a UE that is configured with Default UE credentials, the UE selects an SNPN as ONN and establishes a secure connection with that SNPN referred to as Onboarding SNPN (ON-SNPN).

The present clause specifies security of UE onboarding.

## I.9.2 Authentication

### I.9.2.1 Requirements

The primary authentication shall be performed before UE onboarding is allowed. For primary authentication, the UE shall use Default UE credentials for primary authentication. Credentials or means used to authenticate the UE based on Default UE credentials for primary authentication may be stored within the ON-SNPN or in a Default Credentials Server (DCS) that is external to the ON-SNPN.

The UE shall use Onboarding SUPI and Onboarding SUCI as specified in TS 24.501 [35] during Onboarding Registration.

### I.9.2.2 Primary authentication without using DCS

When the primary authentication is performed between the UE and the ON-SNPN, any one of the existing authentication methods defined in the present document may be used, i.e., 5G AKA, EAP-AKA’ or any other key-generating EAP authentication method (e.g., EAP-TLS).

The choice of primary authentication method used is left to the decision of the ON-SNPN.

Credentials required to authenticate the UE using default UE credentials for primary authentication, are provisioned at the AUSF or AUSF/UDM of the ON-SNPN. The provisioning of this information is out of scope of this document.

### I.9.2.3 Primary authentication using DCS

When the primary authentication is performed between the UE and the DCS, the authentication requirements and procedures defined in clause I.2 for Credential Holder shall apply with the DCS taking the role of the Credentials Holder. When the DCS uses AAA Server for primary authentication, AUSF directly selects the NSSAAF as specified in 23.501 [2]. In this case, the UDM is not involved in the procedure defined in clause I.2.2.2.2, and the step 3 to step 5 shall be skipped. When 5G AKA or EAP-AKA’ is used, the DCS shall act as a AUSF/UDM.

The choice of primary authentication method used between the UE and the DCS is left to the decision of the DCS.

When the primary authentication is performed between the UE and the DCS via the AUSF using EAP-TTLS, Annex U can be used.

### I.9.2.4 Secondary authentication

#### I.9.2.4.1 Secondary authentication using DCS

After successful primary authentication as described in I.9.2.2 (i.e. primary authentication without using DCS), upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with the DCS using Default UE credentials for secondary authentication, as described in clause 11.1.

NOTE: If both primary and secondary authentication use a certificate-based authentication method like e.g. EAP-TLS, and if required by the use case, it is possible to configure the UE with the same client certificates for Default UE credentials for secondary authentication as for the Default UE credentials for primary authentication.

#### I.9.2.4.2 Secondary authentication using DN-AAA

After successful primary authentication as described in I.9.2.2 or I.9.2.3, upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with a DN-AAA server using Default UE credentials for secondary authentication, as described in clause 11.1.

# I.X Access to SNPN services via Non-3GPP access

## I.X.1 Access to SNPN services via Untrusted non-3GPP access

## I.X.2 Access to SNPN services via Trusted non-3GPP access

## I.X.3 Access to SNPN services for N5CW devices

## I.X.4 NSWO support in SNPN

### I.X.4.1 NSWO support in SNPN without CH

### I.X.4.2 NSWO support in SNPN using CH with AUSF/UDM

### I.X.4.3 NSWO support in SNPN using CH with AAA server

\*\*\* END CHANGES \*\*\*